PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 12/24	A1	(11) International Publication Number: WO 98/18235
		(43) International Publication Date: 30 April 1998 (30.04.98)

(21) International Application Number: PCT/US97/19223

(22) International Filing Date: 23 October 1997 (23.10.97)

(30) Priority Data:
08/735,542 23 October 1996 (23.10.96) US

(71) Applicant: MCI COMMUNICATIONS CORPORATION [US/US]; 1133 19th Street N.W., Washington, DC 20036 (US).

(71)(72) Applicant and Inventor: CATERISANO, Terry, A. [US/US]; 1003 Timbercreek Drive, Allen, TX 75002 (US).

(74) Agents: WARREN, Sanford, E., Jr. et al.; Warren & Perez, Suite 710, 8411 Preston Road, Dallas, TX 75225 (US).

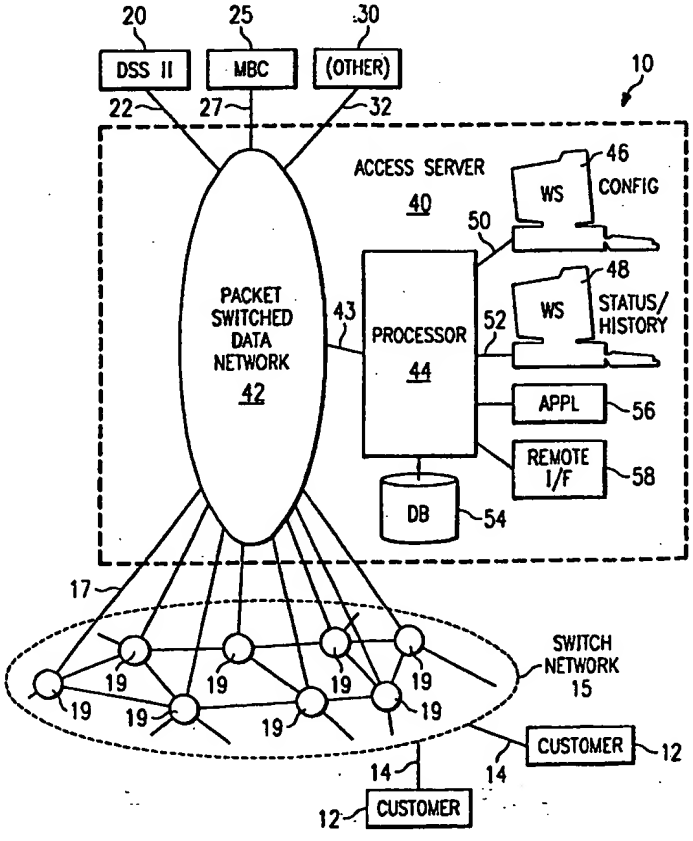
(81) Designated States: AU, CA, JP, MX, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: ARCHITECTURE AND METHOD FOR MANAGING A FLEXIBLE COMMUNICATIONS NETWORK

(57) Abstract

The present invention discloses an architecture and method for establishing one or more variable bandwidth communications channels that provides telecommunication customers with immediate setup of an arbitrary bandwidth connection upon demand. A centrally disposed access server (40) controls all of the switches (19) that form the traffic-bearing network (15) and forms a single portal through which all connection requests are made. Requests from users (12) and network applications are interpreted, validated, translated, and seamlessly delivered to the DXCs by the access server (40). The access server (40) comprises a packet switched data network (42), a processor (44), and several workstations (46, 48) for performing a plurality of customer and network related functions. The access server (40) functions as an intermediatory between a traffic-bearing network (15) and one or more network subsystems (20, 25) which are responsible for allocating the connection based on the customer's request.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

ARCHITECTURE AND METHOD FOR MANAGING A FLEXIBLE COMMUNICATIONS NETWORK

TECHNICAL FIELD OF THE INVENTION

The present invention relates in general to an improved telecommunications system and more specifically to an architecture and method for providing efficient customer setup of an arbitrary bandwidth telecommunications connection upon demand.

BACKGROUND OF THE INVENTION

The Public Switched Telephone Network (PSTN) provides communication services to numerous subscribers. The PSTN is designed for intermittent use by each subscriber because it is neither practical nor desirable to design a network to maintain a constant connection among every possible pair of subscribers. Thus, subscribers effectively share the PSTN by using it at different times and in limited portions of the overall available network bandwidth.

For typical connections, network resources necessary to complete an individual phone call are reserved at the time the call is originated by a calling party. In the telecommunications services industry, a typical subscriber connection consists of one or more telephone lines connected to a central office. The central office, in turn, is connected to a plurality of network switches.

Other types of subscriber connections are often desired. For example, some customers may require semi-permanent connections between particular sites. In such a case, it is often more economical to bypass the central office and connect the sites to each other using a network switch. Such a connection is referred to as a dedicated private line.

A private line is a permanent connection within the network which joins a pair of distant customer sites. Rather than being dialed through a central office to request a network channel, a purely private line is constantly

reserved and available exclusively for a single customer's use.

In addition, customers that need to carry high bandwidth digital data cannot often do so over a single conventional telephone channel. Because such signals are compatible with the high-speed multiplexed telephony signals commonly transported by telephone networks, such customers can use a direct T1 (1.544 Mbps) digital connection to transport such high bandwidth digital data, voice or video.

In addition, customer requirements generally vary between single shared access telephone connections and wide bandwidth dedicated connections. In general, telecommunication subscribers have a spectrum of needs that lie between these two extremes.

For example, in terms of bandwidth, the needs of subscribers typically range from a single telephone voice channel (the equivalent of 64 Kbps) to a Tl line (1.544 Mbps), a T3 line (44.736 Mbps), and beyond. In the interests of scaling services to economically meet customers' individual needs, many options have been developed for allocating bandwidth incrementally. For example, fractional T1 services refer to bandwidth offerings in 64 Kbps increments. In this manner a subscriber does not have to pay for accessing an entire T1 transmission line, when they only require part of the bandwidth. The provider can sell the remaining bandwidth to other such customers.

Variations in the time domain are possible as well. For example, some customers may view constant availability as a critical need, while others can tolerate call setup delays or occasional call blockages in favor of a less expensive solution. Generally, a single telephone line connected to a central office makes a request for network resources whenever a phone call is initiated. If network resources are unavailable, the call is blocked. In contrast, a dedicated line is always connected and available. A compromise between these two extremes is a scheduled shared access line.

A subscriber such as a bank may need a constantly available T1 line for only two-hours every night at a particular time. Thus, the same T1 line can be made available to other subscribers at other times. The arrangement is more cost effective for everyone involved than buying fully dedicated T1 lines that are mostly idle.

To further improve such services, the telecommunications industry is developing techniques for what is known as Bandwidth On Demand (BOD). The goal of BOD is to allow subscribers to instantaneously obtain as much network bandwidth as they need for however long they need it and to have service providers bill them accordingly for the time and bandwidth actually used. Currently, there are several existing and planned techniques for accomplishing such types of flexible connections.

One type of conventional flexible connection is a T1 line with 24 channels (at 64 Kbps each) each of which can be configured as an incoming or outgoing channel. Further, each channel can be configured for a particular type of service, such as a dedicated private line, 800 service, etc.. (depending on the customer). While such a method gives the customer a choice in available bandwidth, the connection typically requires several days or longer to be established by the service provider. Thus, an instant or on-demand connection cannot be established.

Another method gives the customer control of a terminal attached to the provider's equipment in order to reconfigure their communications line based on need. Examples of such services include the Digital Reconfiguration Service (DRS), Dynamic Allocation of Bandwidth (DAB), and Fixed Network Reconfiguration (FNR). These services require a considerable amount of manual intervention and advance planning by the customer prior to connection. Thus, an unsophisticated user cannot easily establish and control the communications link.

The Integrated Systems Digital Network (ISDN) offers a digital subscriber connection with adequate bandwidth to carry several voice and data channels simultaneously. The basic ISDN connection consists of 2 voice channels and 1 data channel while the primary ISDN connection consists of 23 voice channels and 1 data channel. These services

feature fast call setup, moderate bandwidth (up to the T1 rate) and dynamic flexible setup.

ISDN use, however, is limited for several reasons. ISDN services are not readily available in all areas. Additionally, the equipment necessary to facilitate an ISDN connection is typically too expensive for average applications.

Frame relay/cell relay techniques, most notably Asynchronous Transfer Mode (ATM), are expected to pervade the telecommunications market within a few years. These technologies appear promising but their implementation will require further work on standards and large-scale replacement of hardware throughout the network, thus such implementation will be costly.

Providing arbitrary bandwidth on-demand is problematic using existing network equipment in part, because digital cross connects (DXCs) typically support only a limited number of high-speed synchronous X.25 control lines, which are preferred for fast command response. It is desirable to implement a network control design that allows sharing of network control between multiple service-level and network-level applications. Such a design would readily accommodate new applications without an overhaul of existing applications.

Thus, a method and architecture that gives customers a wide range of network resources on an as-needed basis and bills the customer for that resource actually used would

provide great advantages over other methods of flexible bandwidth connections.

SUMMARY OF THE INVENTION

Accordingly, the present invention discloses an architecture and method for establishing one or more variable bandwidth communications channels that provides telecommunication customers with immediate setup of an arbitrary bandwidth connection upon demand.

As such, it is a primary object of the present invention to provide a system architecture that allows a customer to obtain or schedule a connection of almost any bandwidth including DS0, T1, fractional T1, T3 and other bandwidth classes. Custo- mers can request a connection in a number of ways and expect setup times comparable with voice call setup time, that is, within a few seconds.

Another object of the present invention is to provide a system and method for billing customers according to actual use of network resources.

Still another object of the present invention is to provide an architecture wherein network features and services may be added without replacing applications on a widespread basis across the network and in a transparent manner to the customer. In this regard, a centralized access server controls the switches within the traffic-bearing network and functions as a single portal through which all connection requests are made. Requests from users and/or network applications (i.e. for restoration, capacity management, provisioning, etc.) are interpreted, validated,

translated, and seamlessly delivered to the network digital cross connects (DXCs) by the access server.

Yet another object of the present invention is to provide an architecture that is resilient and capable of detecting faults along the transmission path and capable of rerouting the call should a fault be detected. The failover must be transparent to the customer.

An advantage of the present invention is that it allows telecommunication companies to offer ATM-like services well in advance of the availability of such services. The technology used to implement the present invention is readily available and implemented using a modified version of existing equipment and protocols.

Another advantage of the present invention is the increased speed and ease in integrating new network applications because no single application monopolizes the cross connects links (DXC). The present approach also off-loads some of the processing requirements from the DXCs and thereby moves more of the feature implementation into the network control system.

Yet another advantage of the present invention is that DXCs from multiple vendor's equipment can easily be supported by the translation capabilities within the access server.

Still another advantage of the present invention is its redundant distributed design which allows for fast, smooth

cut over of the entire network to an alternate network controller during failure or maintenance events.

For a more complete understanding of the present invention, including its features and advantages, reference is now made to the following detailed description, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE FIGURES

In the drawings:

Figure 1 is a block diagram of an architecture for establishing a flexible bandwidth connection according to one embodiment of the invention;

Figures 2A-2C illustrate the interconnections between a digital network support system (DSS), the MegaHub Basis Controller (MBC), the Digital Cross Connects (DXCs) and the common access server according to one aspect of the invention;

Figure 3 is a high level diagram of a communications architecture for flexible bandwidth management according to one embodiment of the invention;

Figure 4 illustrates the communications architecture between the DSS and the access server according to the invention;

Figure 5 illustrates the redundancy pathway architecture according to one configuration aspect of the invention;

Figure 6 illustrates the mapping of X.25 virtual channels between the access server and other subsystems of the network;

Figure 7 is a process flow diagram of the method used to handle network control messages according to the invention;

Figure 8 is a block diagram of the customer setup and provisioning functions according to one embodiment of the invention;

Figure 9 is a graphical user interface for a CVNM tool which may be used to select origination/destination city pairs for path connection.

Corresponding numerals refer to corresponding parts in the figures unless otherwise indicated.

DETAILED DESCRIPTION OF THE INVENTION

In part, the present invention is an improved telecommunications system and architecture that provides customers with immediate setup of an arbitrary bandwidth connection upon demand. A centrally disposed access server controls all of the switches that form the traffic-bearing network. The access server is the single portal through which all connection requests are made. Requests from users and network applications are interpreted, validated, translated, and seamlessly delivered to the DXCs by the access server.

Referring now to Figure 1, a block diagram of a telecommunications network for flexible bandwidth management according to the preferred embodiment of the invention is shown and denoted generally as 10. As illustrated, network 10 comprises an access server 40 that is centrally configured between the traffic-bearing network 15 and the Network Support System (NSS) 20, the Cross Connect Controller (CXC) 25 and some other network related functionality 30.

The traffic-bearing network 15 may comprise any one of the known and existing switched data networks capable of carrying signals of varying bandwidth and densities. Examples include Public and Private Data Networks (PDNs), local exchange networks and still others as is appreciated by those skilled in the art. Network 15 is shown to comprise numerous interconnected switching nodes 19 each of

which has a control link 17 coupled to the access server 40 which, in turn, coordinates the delivery of switching commands within the entire traffic-bearing communications network 15. Likewise, network customers 12 have access to the switch network 15 via links 14.

The core of the access server 40 comprises a packet switched data network 42, a processor subsystem 44 and several workstations 46 and 48 and corresponding interfaces 50 and 52. In practice, the network 42 may be an X.25 packet switched network implemented using, for example, commercial off-the-shelf (COTS) routers like the DynaStar 200 manufactured by Dynatech Corporation.

In one embodiment, processor subsystem 44 comprises one or more Alpha processors made by Digital Equipment Corporation and has at least one communications link 43 coupled with the network 42. The processor subsystem 44 also has access to a database 54 for storing a variety of network related information to support the various functions. Examples include control link information, DXC node type, switch, router and channel configuration information among other as would be appreciated by those skilled in the art.

Various subsystems that would normally exercise direct control over the traffic-bearing network 15 are represented by blocks 20, 25, and 30. In accordance with the present invention, these blocks 20, 25, and 30 are COTS subsystems that have been modified as described below. In this regard,

Figures 2A-2C illustrate the progression of control arrangements used to describe the modifications of the subsystems 20, 25, and 30, according to the preferred embodiment of the invention.

In Figure 2A, the provisioning subsystem 20, preferably having a graphical user interface (GUI) front-end, is shown connected directly to a traffic-bearing network 15 of switches, as depicted by the DXCs 70. The provisioning subsystem 20 can be a Digital Support System made by Prism Systems that is generally used as a network management system for monitoring the state of a network 15.

In accordance with the present invention, the NSS 20 is adapted to perform two functions. First, the modified NSS 20 provides a visual workstation from which to establish the end-to-end connection and administer customer privileges, according to the present invention. The second function performed by the modified NSS 20 is to provide a real-time, fine-grained view of the actual routing of traffic in response to connection requests. In addition, the NSS 20 performs enhanced network management functions for established calls.

Figure 2A also shows CXC 25 which in one embodiment is a modified version of a MegaHub DEX 600E (MegaHub) switch made by Digital Switch Corporation. The CXC 25 is used to accomplish usage-based billing, alarm filtering, and centralized connection setup among other similar network control functions.

In accordance with the present invention, a MegaHub 25 is modified by replacing the internal switch fabric with X.25 control links to the network DXCs 70. In this manner, the modified MegaHub 25 handles the entire network 130 as if it were a single switch matrix. The MegaHub 25 so modified is referred to as the MegaHub BASiS Controller (MBC).

Various methods can be used to modify the internal switch fabric of the CXC 25. Specific implementations of such modifications will be apparent to persons skilled in the relevant art.

The MBC 25 provides for a wide variety of methods to setup a connection. For example connections can be setup using Dual Tone Muiltifrequency (DTMF), dial-up lines, dedicated lines, or in-band signaling methods. Other means contemplated for signaling connection setup include SS7, Internet and others which are apparent to those skilled in the art.

Regardless of how the CXC 25 is implemented, the subsystems 20 and 25 are conventionally applied separately. That is, prior to the present invention, there has been neither a motivation nor a means for integrating the operation of these two types of subsystems, such as the subsystems 20 and 25.

Furthermore, a general technical barrier to such integration has existed in that each DXC 70 generally supports a limited number of control links. In addition, it is common to use redundant connections from a given

supervisory control subsystem to improve network reliability and increase robustness. Thus, conventionally it has been problematic to have multiple subsystems controlling a common set of network switches 15. However, for various reasons, it is desirable to have two or more subsystems, such as 20, 25 or 30 control a common set of network switches 15.

For example, the integration of the operation of subsystems 20 and 25 serve to solve a conventional problem associated with the field of network control that relates to adding new functionality 30 to the network. Adding new functionality 30 generally involves modifying and adding software to both the DXCs 70 and the control elements such as 20 and 25, which are already driving existing applications. Thus, in order to add new functionality 30, several applications are forced to coexist within a single subsystem, such as the subsystem 20, because DXCs 70 are typically driven by a single supervisory subsystem.

However, as will be apparent, by sharing network control between multiple subsystems 20 and 25, new functionality 30 can be accommodated without an overhaul of prior software. For example, the application software for a new function can reside in any other subsystems 30 that have shared access to the DXCs 70. Thus, the integration of the two subsystems 20 and 25 is particularly advantageous.

Figure 2B depicts an example of how the subsystems 20 and 25 can be further modified and applied to operate upon a common network 15 in accordance with the present invention.

As shown, the subsystems 20 and 25 are modified so that they communicate with each other. Within each subsystem 20 and 25, a communications process is added (20a and 25a, respectively).

In addition, two communication channels 72 and 74 are used to join the two subsystems 20 and 25. In a preferred embodiment, these communication channels 72, 74 take the form of an SS7 Transaction Capability Application Part (TCAP) message format to comply with prevalent standards although other formats may also be used. In this manner, the NSS 20 may send call setup information to the MBC 25. The MBC 25, in turn, causes a connection to be formed within the network 15. Likewise, the MBC 25 can send unsolicited path change information to the NSS 20 so that the latter may maintain an up-to-date representation of what is connected within the traffic-bearing network 15 and perform real-time alarm and performance monitoring.

Various methods can be used to implement the communication processes 20a and 20b and specific implementations of such modifications as described above, will be apparent to those skilled in the art.

Another modification of subsystems 20 and 25 is shown in Figure 2C wherein the packet switched connections 76 and 78 from the subsystems 20 and 25, respectively, which are conventionally connected directly to DXC 70 control links, are instead connected into a common access server 40 according to the present invention. In this manner, both

subsystems 20 and 25 may act upon a common set of switches in the traffic-bearing network 15.

It is a distinct advantage of the present invention that numerous subsystems, such as subsystems 20 and 25 and/or applications within such subsystems, may each act upon the network 15 without requiring an awareness or regard for one another. This feature is useful for providing fast, efficient, and simple integration of applications upon a common network 15.

Note that the interconnection of the two subsystems 20 and 25 as described above, via the direct connections 76 and 78 are accomplished via the common access server 40 as depicted by the PVC/SVC channel 80. If the subsystems 76 and 78 were directly connected, as shown in Fig. 2B, the first aspect of interoperability as described above can be practiced in the network 15 independently of the access server 40.

There is an additional practical benefit in using the access server 40 as an intermediate between the subsystems 20 and 25. The NSS 20 generally operates its packet switched links in a switched virtual call (SVC) mode. This means that a connection or session is established for each message that traverses the link. This is adequate for intermittent or low volume use where response time is not critical. On the other hand, the MBC 25 operates some of its packet-switched connections in a permanent virtual circuit (PVC) mode. In a PVC mode, a session is established

once and then used for all subsequent message communications.

The PVC mode is preferred for continuous, high-volume use when a session setup for each message would incur too much delay. Therefore, for practical reasons, the common access server 40 is also conveniently used as a platform for adapting between the mixture of SVC and PVC links that are prevalent in telecommunications hardware and applications.

Referring back to Figure 1, the NSS 20 and the MBC 25 are shown attached to the packet switched network 42 within the common access server 40 via links 22 and 27, respectively. Other subsystems, represented by the block 30, may similarly be connected to act upon the traffic-bearing network 15. In this manner, new subsystems that are developed in the future, as well as legacy subsystems which customers use to exercise limited configuration and control, are easily accommodated by the network control system of the present invention.

As disclosed, the subsystem 20 may be implemented using Prism's Digital Support System (DSS) which may be configured to perform various network management functions. While the functions and configuration settings of a DSS 20 may vary, as is understood by those skilled in the art, the following description highlights various features of a DSS per one embodiment of the invention:

DSS 20 SPECIFICATION, FEATURES AND FUNCTIONS ACCORDING TO ONE EMBODIMENT

The DSS 20 can be implemented through a number of independent and yet operationally integrated software feature groups. DSS 20 monitors and correlates functions among the feature groups. A common application interface ensures all parts of DSS function as a single entity even if individual modules are installed at physically separated locations. With unified visibility on DSS 20, an operator can respond quickly without the need to perform tedious operational duties on duplicated hardware that would otherwise be required.

DSS-II APPLICATIONS

Operator Workstation (OWS)

Using a standard OSF/Motif compatible X-terminal or workstation with a TCP/IP interface, an operator can log on from any location and simultaneously access different applications of DSS 20 or any other X-window compatible OSS through point-and-click interactions.

Event Logging (ELS)

DSS 20 allows customization of event log displays on an ad hoc basis according to operator instructions. Users can obtain precise and quick isolation of real-time and historical information. An operator can categorize events by equipment and transmission facilities along with alarm severity. New alarms are highlighted for quick review until they are acknowledged. In this way, an operator can easily

identify potential network problems or any log on attempts by unauthorized personnel.

Service Inventory Management (SIS)

An intelligent Ingres relational database management system is employed in DSS 20 to improve user querying of the inventory system. Key inventory information such as circuits, equipment and customer information are synchronized with other DSS feature groups, thus allowing better management of the network with consistent and updated information. In addition, the inventory database correlates bandwidth and path objects with customer data to provide virtual network management.

Application Management (APM)

DSS 20 operates on a scalable LAN architecture. DSS 20 can monitor feature groups which are distributed across multiple host systems and, if so equipped, to prevent a total failure. DSS 20 can maintain standby copies of each software module on optional redundant host hardware such that an application can be quickly restored upon primary failure or during hardware/software upgrade. Database information can be maintained simultaneously on multiple hardware systems to ensure configuration integrity.

Connectivity Management (lMS)

DSS 20 employs connectivity management software which supports creation, removal, non-contending bandwidth allocation and pre-plan restoration of end-to-end DSO, nxDSO and DS1 circuits. A central and unique feature is Customer

Virtual Network Management (CVNM) which provides fine-grained partitioning of bandwidth based on customer identifier.

Customer Network Status Display

DSS 20 correlates with the inventory database and the event log system to support graphical status display of a customer virtual network on an industry standard PC. This feature is used in the provisioning of customer services.

External System Interface (ESI)

Integrated access to DSS 20 from embedded Order Entry and Provisioning systems can be developed based on an external system interface. The integration of DSS 20 with existing or upcoming operational support systems eliminates system boundaries and duplicated hardware to provide a more efficient operation.

DS1 Management

In one embodiment, a total of six (6) Sun SPARC 10 servers are used wherein four (4) of these are SPARC 10 model 51's that are configured for host applications. The remaining two are SPARC 10 40's that are configured for communication processing. Two (2) of the four (4) application servers (Type A1) are configured for database applications, and each equipped with 256 MB memory as well as 6.3 GB disk. The other two (2) (Type A2) are configured for other applications, and each equipped with 256 MB memory and 4.2 GB disk. Resilient operation will be provided, with

an active and a standby copy of the Ingres RDBMS and each application subsystem deployed among the four servers.

The communication servers support network element communications. Each system is equipped with 224 MB memory and 2.1 GB disk. The host systems communicate to the network elements on X.25. This is achieved by a synchronous RS-449 ports on the servers.

Also, in one embodiment, five (5) Sun SPARC LX workstations provide the user interface for database management, system administration, and other usage where system response is important. All servers and workstations may be interconnected via an Ethernet LAN system, with TCP/IP communication.

An NSD/PC terminal allows a CVNM customer to monitor his dedicated network from a personal computer at the customer premises. Each of the four (4) application servers has eight (8) asynchronous ports for text terminal, printer, NSD/PC and other peripherals.

DS1 Path Provisioning

DSS 20 supports definition of DS1 rate paths in the DS1 network. In this regard, DS1 paths are transported through the network on any hardware compatible 1/0 DCS switched facility.

DSS 20 supports definition of DSO and n*DSO rate paths in the DS1 network. DSO paths are transported through the network on any 1/0 DCS switched facility. The DSS administers signaling for voice and data paths.

DDS Path Provisioning

DSS 20 supports the definition of 2400, 4800, 9600 and 56000 bps DDS paths in the DS1 network. These paths may be transported through the network on any 1/0 DCS switched facility. Additionally, DSS 20 supports the subrate multiplexing of these circuits at any 1/0 DCS suitably equipped for the operation.

Multipoint Path Provisioning

DSS 20 supports definition of DDS MJU and data polling DMB paths in the DS1 network. DSO paths may be transported through the network on any 1/0 DCS switched facility. Internal cascading of multipoint circuits will only be supported for MJU circuits. Other types of multipoint circuits are not supported, including peer to peer symmetrical bridging.

Bandwidth Partitioning

DSS 20 partitions DSO bandwidth based on customer identifier. Bandwidth associated with a specific customer identifier may only be used in paths defined for that customer. The allocation of bandwidth in this manner is typically performed by telco users. Specific users may be assigned the privilege of using pre-assigned Bandwidth On Demand (BOD) pools during path definitions. The privileged telco user is responsible for assignment of bandwidth. This includes Bandwidth on Demand (BOD) pools.

Customer Partitioning

DSS 20 supports information partitioning in specific DSS operations based on the customer's defined virtual network. For example, query operations can be restricted based on customer identifier.

Partition Security

DSS 20 enforces the virtual network partitions and prevent unauthorized users from seeing across the partition boundaries within 1MS, ALS and ELS applications. DSS 20 provides a user specific profile, controlled by the system administrator, that specify valid customer IDs for the user and assign privileges to perform DSS operations on a per command basis.

Bandwidth On Demand

DSS allows DSO bandwidth to be associated with specific bandwidth on demand (BOD) pools. Specific users are granted access to specific BOD pools for path definition. BOD bandwidth is returned to the BOD pool when the user discontinues its use (ie. schedule completes and path is removed from service). Typically, BOD pools are setup by telco users and CVNM users schedule DOD use of specific amounts of bandwidth.

Partitioned Alarm Display

DSS provides a customer partitioned display of facility alarm events affecting a customer virtual network.

Platform

DSS software executes under the UNIX operating system.

In one embodiment, on a SUN 4 platform using SUNOS (Solaris 1) is used although other X-Windows compliant workstations may be used. A database system, such as the INGRES RDBMS, may be installed on the DSS platform. DSS 20 shall require that VI Corpis DataViews be installed on the DSS platform. DSS 20 may be installed on a multiple SUN 4 computer platform co-resident on an ethernet LAN.

Site Resilience

DSS applications provide reliable operation in a distributed non fault-tolerant multi-processor platform. Each DSS application can be constructed with a common Remote Procedure Call (RPC) based inter-process communication API that enables a client-server application architecture. Application client components locate (transparently to the user) their corresponding active server components upon start up and behave gracefully in the face of non client (ie LAN, server platform, server application) DSS outages.

Eligible application server components have at least one active instance and one standby instance on different computers in the platform. Change over to the standby instance of any server is controlled by the application manager.

The time for each DSS application to change over to the standby instance is application specific. Typically, an application shall change over in under 15 minutes. DSS application components can be deployed on any of the

computers of the platform to achieve improved performance and reliability.

DBMS

In one embodiment, Ingres relational DBMS is used for storage of the network management inventory information. ANSI standard SQL is used by DSS software to access these inventories. Also, in another embodiment, DSS 20 uses the Raima DBMS product (formerly called DBVista) for storage of DSS internal events and network generated events.

Data Communications

In one embodiment, DSS 20 is configured with two Sun SPARC 10 communications engines to support initial efforts to control approximately 86 DSC DEX CSLL nodes as well as interconnecting the DSS and MBC-2 systems. DSS communicates through access server(s) designed to interface to each system's native X.25 links and route X.25 virtual channels serving the different applications.

Each DSS communications system runs SunLink X.25 communications software and supports 2 four-port HSI cards that plug into the system SBUS. Each port supports an RS-449 physical interface.

Each DSS communications server supports a minimum of two (2) HSI cards supporting 4 ports each. At least one more can be added to each server as needed. Depending on the number of spare SBUS slots, more HSI cards may be added to each server.

Each DSS communications supports a minimum of four (4) 56 Kbps X.25 links. This allows the DSS 200 to use a pool 8 physical links with 256 channels per link to establish any virtual control channel.

The DSS 20 automatically establishes Switched Virtual Circuits (SVCS) to any defined DXC and MBC channels. If an SVC fails, the server will attempt to re-establish it. If the physical 56 Kbps link fails, all sessions on that link will be restarted on other physical links. In one embodiment, each DSS communications supports a minimum of 256 Switched Virtual Circuits (SVCS) per X.25 physical link allowing up to 1024 SVCs per communications server.

Additional communications servers can be added easily to support larger link capacity and throughput requirements. Thus, the DSS communications system is scalable and can grow as needed to support additional nodes, higher throughput and performance.

Method of Operation

In the preferred embodiment of the invention, DSS 20 supports remotely routed circuits which are tracked within the database as described above. A CVNM tool will extract from the SOT a node name; the node must be a multiplexer. Also, if the node type is valid the DSS 20 will prepare a list of 10-digit MBC ports defined at that node. This list will only show those ports for which the user's profile allows (e.g ports for other customers will not be displayed). The CVNM tool will allow the user to select a

single 10-digit port per node. Two nodes are required to be selected - one for the originating and one for the terminating end of the circuit.

The user can select a node in a variety of ways. Using the ALS, the user could click on the node. Nodes are not displayed on the user's ALS screen if no circuits for their profile have defined. Users can also select nodes via the SOT lookup method or via the SIS. When both nodes have been selected and their ports selected the user will be presented with the option of placing the circuit into service or removing from service immediately. If a circuit is placed into service then the circuit record will automatically generated via the path generation software described above within a short period of time.

The list of 10-digit ports available at the node will be selected from the database each time the user selected a node. Thus, the user does not need to maintain his own copy of the 10-digit ports available to the user.

The access server 40 also drives a number of interfaces other than the subsystems 20, 25 and 30, and the traffic-bearing network 15. In particular, as shown in Figure 1, a configuration workstation 46 is shown connected to processor 44 for the purpose of allowing network personnel to view or assert information about what subsystems 20, 25 and 30 and other network elements connected to the access server 40. This information is stored in the database 54 and may

further include the capabilities and protocols appropriate to each entity attached via packet switched network 42.

The status/history workstation 48 is also shown coupled to the processor 44 for the purpose of displaying the operational state of the packet switched network 42 and all links connected thereto. This status/alarm monitoring can encompass all software applications, hardware devices, and router ports in the realm of the access server 40.

The application block 56 in Figure 1, represents a functionality, such as a software process or the like, that can act directly through the access server 40. One of the uses contemplated for such an application 56 are uploading/ downloading operating software, database contents, commands, and status indicators, to and from the traffic-bearing network switches 15.

The remote interface block 58 represents a connection that allows remote processes to access many of the same functions within the access server 40 as are provided through workstations 46, 48 or application 56. Thus, remote control and monitoring of the network controller can be accomplished.

Those skilled in the art will immediately appreciate that various implementations of the access server 40 may be achieved. The following description of the access server 40 conforms to one contemplated embodiment and highlights, without limitations, various aspects of an access server according to one embodiment:

ACCESS SERVER DESCRIPTION AND FUNCTIONAL SPECIFICATION ACCORDING TO ONE EMBODIMENT

The objective of the access server 40 is to route messages through virtual channels using X.25 concentrator devices and low level X.25 router equipment without introducing any delay in the end to end message path. In this regard, most of the virtual channels (see Figure 6) are routed through the access server 40 point to point and do not require any processing other than routing. This routing can be handled completely by the X.25 communications servers and do not require any system CPU utilization. Limiting message delay is most critical in the routing and processing of the DXC binary messages.

Thus, in the preferred embodiment the access server 40 introduces nearly zero delay in any end to end virtual message path that does not require additional application processing. Likewise, the access server 40 introduces no more than a 100 millisecond delay to the end to end message paths that require application processing such as database updates and message logging. This requirement applies specifically to the binary and ASCII connection and disconnection control channels.

The access server 40 supports a minimum of 120 DXC nodes and may be expanded to add additional DXC nodes as needed. The access server 40 continuously monitors all X.25 physical links and virtual channels and report alarms to a Network Management System (NMS) when a failure occurs.

A major alarm shall be reported when a single link failure is detected and a critical is reported when both (redundant) link failures are detected. Alarm idle messages are reported when link connectivity is restored.

The access server 40 periodically attempts to restart any virtual channels that have failed. The interval for the periodic retry shall be configurable by the administrator ensuring that once a physical failure has been corrected that further manual intervention is not necessary to restore the communications channel.

Operational Requirements

The access server 40 system software consists of operating system services which provide the background for the other application software layers. These services include the following:

- System Security Services System Management Services

The access server 40 provides a means to ensure the protection of the system from unauthorized access or interference.

- System backup and restoral facilities.

For disk and magnetic tape operations, the operating system software provides for device control for disk, tape and print device formatting, and mounting.

- Management of disk space, purging, sizing and process quotas.
- Tools for analyzing disk and magnetic tape errors.

- Batch and print operations managing process queues and jobs.

- Maintaining system log files and providing dump file analysis.

- System generation and boot process - Installing device drivers, shared memory segments and processes.

- Monitoring and management of system performance.

- Application software scheduling and monitoring

The access server 40 maintains statistical information (e.g. failure counts, retry attempts) for each external interface link enabling users to monitor link performance and view link status.

System Interface Requirements

The access server 40 adapts to the native physical interface of each external system connected to it. Each of the external systems that the server communicates with are existing systems and have their own specific physical interface requirements. The access server 40 accommodates each native interface and requires no development to any of the external systems in order to communicate through the access server.

The access server 40 supports the following physical data communications interfaces to the specified systems:

- X.25 SVCs - DSS-II
- X.25 PVCs - MBC-2 (DXC and TCAP links)
- X.25 SVCs - DRS
- X.25 SVCS - DSC DEX CSLL DXCs
- TCP/IP - Billing System
- Ethernet - NMS

. Ethernet - Access Server

The access server 40 supports the routing of the following communications protocols:

. DSC Binary DXC protocol
. PDS Snyder ASCII protocol
. TCP/IP
. Decnet
. X.25

The access server 40 provides the routing of message traffic needed to support the integration of component systems enabling the following data flows:

System			Message Type
DSS-II	< --- >	MBC-2	Binary SS7 TCAP messages
DSS-II	< --- >	DSC 1/0 DXCs	ASCII PDS messages
DRS	< --- >	DSC 1/0 DXCs	ASCII PDS messages
MBC-2	< --- >	DSC 1/0 DXCs	Binary DXC messages
Server	< --- >	NMS	System alarm messages
Server	< --- >	Billing	Call Detail Records

DSS 20 Interface Requirements

The DSS 20 system is configured with two Sun SPARC 10 communications engines to support DSC DEX CSIL nodes as well as interconnecting the DSS 20 and MBC-2 systems. DSS 20 will communicate through the access server 40 designed to interface to each system's native X.25 links.

Because of the duplicated nature of the platform components, the DSS 20 communications are directly connected

to each access servers (see Figure 3 and 5), one collocated and one distant.

The access server 40 provides physical link redundancy (see Figure 5) and routing of the virtual channels (see Figure 6) towards the network DXCs and MBC-2 systems. DSS 20 will monitor link failures and report loss of communications.

Each access server 40 supports a minimum of four (4) 56 Kbps X.25 DSS-II control links. This allows the DSS 20 to use a pool of 8 physical links with 256 channels per link to establish any virtual control channel to the DXCs and MBC-2 systems.

Each access server 40 supports a minimum of 256 Switched Virtual Circuits (SVCS) per DSS-II X.25 physical link allowing up to 1024 SVCs per DSS-II communications server. The access server 40 supports a CCITT compliant X.25 communications stack and performs the function of a standard Packet Switching Data Network (PSDN). No proprietary Q-bit session layer manipulation is required to interface to the DSS-II communications subsystem.

In one embodiment, the access server 40 allows 4 SVCs per DXC node from the DSS-II to be routed to 4 DXC ASCII SVCs controlled by the access server 40 and allows a minimum of 2 SVCs to be routed from the DSS-II to the MBC-2 TCAP gateway interface PVCs.

Turning to Figure 3, a high level block diagram of an integrated bandwidth allocation system according to the

invention is shown and denoted generally as 100. In particular, dual and redundant systems 102, 104 are provided which allow crossover operation of each system for the entire network.

With respect to the left side 102, Figure 3 illustrates that customer premise equipment (CPE) 105 is used to gain access to the digital reconfiguration service (DRS) processor 109 via access terminal 107. As is known in the art, DRS is a network management system application that is designed to reconfigure a customer's portion of the connection and to configure temporary bandwidth when the customer needs additional capacity.

As shown by Figure 3, the left side 102 has a DRS processor 109 are communicably linked to an access server 113 which provides various channel concentrating and routing functions as herein described. In one embodiment, access server 113 and its redundant counterpart 115 comprise X.25 router equipment and DEC Alpha Processors which provide shared access to the network 111.

Redundant access servers 113 and 115 are communicably coupled to each other via links 114 and 116. Likewise, the access servers 113 and 115 are linked to the customer management service (CMS) processor 117 via control links 119. The CMS platform 117 is an entryway into various customer-related features and functions, such as customer orders, partitioning, message routing and other similar and related customer-related operations.

Turning now to Figure 4, the architectural interface between the Digital Network Support System (equivalent to DSS 20 in Figure 1) 155 and access servers 159, 161 is shown. Figure 4 shows that a plurality of application servers 155, which collectively form an operable DSS, are provided upon which the various system wide applications are executed. Server operations include provisioning of end-to-end circuits, static or dynamic route selection, scheduled circuit reconfiguration, monitoring of network performance, partitioning of network resources, multi-level security access, multi-vendor support, disaster recovery and alarm management, customer virtual network management, graphic display of network status and interactive or batch processing of command files among others.

As shown, the application servers 155 are communicably linked via LAN link 157 to communication servers 159 and 161 which, in turn, provide the control and command paths to access servers 163 and 165. In this regard, servers 163 and 165 are the functional equivalent of access server 40 of Figure 1 as previously described.

In one embodiment, each access server 163 and 165 supports a minimum of four (4) control links. Thus, each access server 163 and 165 can route X.25 virtual channel concentrating and routing functions to the application servers 155. The communications pathway is provided by communications servers 159 and 161 and link 157 which in one embodiment is a TCP/IP channel.

Each access server 163, 165 supports a CCITT compliant X.25 communications stack and performs the function of a standard packet switch data network. In this way, the access servers 163 and 165 can allow various SVCs per DXC node from the application servers 155 to be routed to DXC ASCII SVCs controlled by the access servers. In short, the access servers 163 and 165 form a transmissive non-interruptive control path between the data traffic-bearing network 15 and the network support system in place.

Turning now to Figure 5, a communications architecture 200 illustrating the redundancy feature according to one embodiment of the invention as shown. The goal of architecture 200 is to provide high reliability to redundant paths between the various applications and DXCs in the network. As illustrated in Figure 5, 2 MBC processors 205 and 207 are communicably linked to one another via signal link 209. This provides dual and independent network controllers which can each separately operate and handle the whole load of the entire network should one side of the network control systems experience a catastrophic failure in equipment.

As shown, remote switches 211 and 213 provide physical links to opposite sides of the network control systems and give each side the ability to switch over should a fault occur. The switch layer 215 couples the MBC processors 205 and 207 to access service layer 217 which comprises a plurality of packets switch data components including

concentrators 230 and access servers 233. A wide area network 219 is interspersed between the respective sides of the architectural system 200 providing a communications path at the server level 217. Finally, the digital cross connect layer 250 provides the link to the corresponding data traffic network.

As stated, one purpose for the access server 40 is to route system wide messages through virtual channels using X.25 concentrator devices and low level X.25 router equipment (layer 217) without introducing any delay in the end-to-end message path. In this regard and according to one embodiment, most of the virtual channels routed through the access server are point-to-point and not requiring any processing other than routing. This routing can be handled completely by the X.25 communications servers (159 and 161 of Figure 4), thus not requiring any further access server utilization. The access server layer 217 must intercept digital cross connect connection messages from layer 250 and determine connection status, deliver responses and queue them for update processing.

In short, Figure 5 depicts a high degree of redundancy among various processors and connecting links. In particular, a primary level of redundancy is afforded by the T1 links between the left and right halves of Figure 5. A secondary level of protection among access server processors of layer 217 is provided by the WAN 219. Finally, the X.25

routers 230 are extensively cross-connected so that a failed router or link can be readily bypassed.

This design assures a highly robust architecture for distributing control information to the DXC layer 280. In fact, the system is designed to allow two (or more) MBCs 205 and 207 to control a network. As an important advantage of the present invention, these MBCs 205 and 207 may be geographical separated so that, in the event of a catastrophic failure of one MBC, control of the entire network can readily be assumed by the other MBC without any service disruptions. In Figure 5, SS7 signaling links 209 are shown connecting the two MBCs 205 and 207. This is done to maintain an accurate database of the state of the network at both locations.

Turning now to Figure 6, the mapping of the various X.25 virtual channels between each access server 159 and 161 and other network subsystems is shown and denoted generally as 275. Figure 6 shows the device virtual channels 280 which are routed to the access server side 285 on a point-to-point basis eliminating unnecessary delays. In one embodiment, the access server side 285 introduces no more than a 100 millisecond delay to the end-to-end message path that requires application processing such as data base updates and message logging. This requirement applies specifically to the binary and ASCII connection and disconnection control channels.

In another embodiment, the access server side 285 is designed to support a minimum of 120 DXC nodes and may be expanded to add other nodes as needed. In this regard, it should be understood that the access server side 285 of Figure 6 illustrates the signal pathway traffic incoming and outgoing the physical access server 40 in Figure 1 as well as redundant access servers 113 and 115 of Figure 3.

Other virtual channels between DSS 290, DRS 295, DXC 300, DXC manager 305 and TCAP gateway 310 are illustrated showing virtual channel paths and link designations according to the contemplated embodiment.

Access server side 285 provides the routing of message traffic needed to support the integration of various network wide components according to a set routing process which is denoted in Figure 7 as 300. Process 300 with step 305 when the access server initializes the various links to determine whether the links are active and operational.

Next, in step 310 the access server examines the status of the various virtual channel connections and reports the status to the network support system. At this point, the access server waits to receive the message along the link, step 315, and verifies the validity of any messages to assure an appropriate command or control is being sent, step 320. As shown, as long as a message is not received, process is directed to step 317 to examining the status of the various links across the network.

When a valid message is received, process flow is directed to step 330 wherein the access server collects the message source and designation input and looks up any translation of instructions specific to the message received, step 330. Next, in step 335 the message is interpreted and transformed as needed and a route is selected to determine the best way to send the message to its intended destination, step 340. The message is sent and when sent successfully process flow is directed to step 317 wherein the access server reevaluates the status of all links waiting for the messages.

On the other hand, where a message is not successfully sent and all possible routes have been exhausted, step 350, and a rejection message is sent, step 355, to the message source and the command or message transfer is aborted. Should other routes be available, in step 355 the access server looks for other links and selects the best route for the intended destination, step 340. This evaluation may involve testing for protocol adherence, access privilege, valid destination references and other qualifiers as is appreciated by those skilled in the art.

Turning now to Figure 8, the method of selecting a flexible bandwidth resource is shown and denoted generally as 375. Process 375 starts when a customer or service provider places an order for a bandwidth resource 380 which, in turn, is routed through a circuit provisioning process 385. In the preferred embodiment, the order is

instantaneously transferred to the circuit provisioning process 385 allowing an on-demand selection to be made.

Next, the customer order is directed towards a provisioning system 390 which receives the request in real time and updates the appropriate customer services data bases to ensure the customer has the authority and access to the requested bandwidth resource. If so, process flow is directed toward step 395 wherein the call and billing records are set up by the network using the appropriate control links. Also, network maintenance may be required 400 to assure correct signaling of the point-to-point connection as well as the quality of the link.

Finally, process 375 is directed to setting up the call 405 which establishes the connection and gives the customer exclusive use of the end-to-end transmission channel at the requested time and bandwidth.

Turning now to Figure 9, a screen 425 front end graphical user interface for a connection set-up utility is shown. Screen 425 may be used by a telecommunications customer or other user to set up a point-to-point communications channel which will enable a connection between any two points on the network. For example, the customer could use screen 425 to set up a communications link at a given time and date and for a given duration assuming the customer has authority to use the service. In this way, a customer can configure a high speed data transfer between any two points on the network, such as a

video conference, a remote data bases search or other similar unscheduled, high performance data transfer.

As shown, screen 425 is split into a left side 430 and a right side 435 which in one embodiment correspond to origination and terminating points for the connection. On the origination side 430 a customer is given the choice of various locations from which to originate the call. A unique ten digit identifier and description field 434 is provided corresponding to each available origination site.

Likewise, a menu 437 of available for destination points on the right side 435 of screen 425 which allows the user to select from a plurality of available terminating points for the call. As shown, each terminating point has a four digit identifier and description 439, corresponding to end points on the call connection path. A confirmation box 440 is provided allowing the customer to configure the end-to-end path for the connection used using the specified service and at a specified time and/or date. It should be readily understood that screen 425 is illustrative of one of many possible embodiments and that the features illustrated encompass one of many possible solutions to the same problem.

While this invention has been described in reference to illustrative embodiments, the description is not intended to be construed in a limiting sense. Various modifications and combinations of the illustrative embodiments as well as other embodiments of the invention will become apparent to

persons skilled in the art upon reference or description. It is, therefore, intended that the appended claims encompass any such modifications or embodiments.

5

What is claimed is:

1. A network architecture for establishing variable bandwidth communication channels upon demand, said architecture comprising:

a traffic-bearing network having a plurality of nodes linked to each other via a plurality of transmission paths, said nodes forming local hubs connecting a plurality of end users;

an access server coupled to said traffic-bearing network via a first plurality of communications links for receiving messages from said end users; and

a network support system communicably linked to said access server via a second plurality of communications links, said network support system configured to perform a plurality of network management functions.

2. The architecture of Claim 1 wherein said access server further comprises:

a packet switched data network coupled to said first plurality of communications links for receiving messages from said end users;

a processor subsystem communicably linked to said data network;

a database coupled to said processor and storing a plurality of end user and network related information; and

a group of workstations configured to provide a plurality of network configuration functions and

status/history functions, said workstations communicably linked to said processor.

3. The architecture of Claim 1 wherein said network support system further comprises an application for initiating call setups and administering customer privileges.

4. The architecture of Claim 3 wherein said network support system further comprises an application for obtaining a near real-time view of network routing traffic in response to connection requests.

5. The architecture of Claim 1 further including a cross connect controller communicably linked to said access server via said second plurality of communication links.

6. The architecture of Claim 5 further comprising communications channels coupling said cross connect controller and said network support system.

7. The architecture of Claim 5 further including a plurality of switched X.25 virtual circuits forming a signal path between said access server and other subsystems of said network architecture.

8. The architecture of Claim 2 wherein said packet switched data network include a plurality of X.25 concentrators and low level X.25 routers for transmitting X.25 formatted messages along said network architecture.

5

9. The architecture of Claim 7 wherein the access controller introduces a near zero delay into the X.25 virtual circuit message paths.

10. A central access server for establishing a point-to-point communications channel in a telecommunications network said network comprising at least one traffic-bearing switched network, one network subsystem for provisioning available network resources and one cross connect controller, said access server comprising:

a packet switched data network communicably linked to both said telecommunications network and said network subsystems via a plurality of switched virtual circuits;

a processor subsystem coupled to said packet switched data network via a first communications link supporting a switched data protocol for receiving said messages originating from said telecommunications network;

a group of workstations linked to said processor subsystem and containing a plurality of network related applications for performing network related functions; and

a database structure coupled to said processor for storing a plurality of network related information.

11. The central access server of Claim 10 further including:

an application program for uploading or downloading operating software, database contents, commands, and status indicators to and from said traffic-bearing switched network; and

a remote interface that provides access to functions within said access server, said functions provided by either said workstations or said application program.

5

12. In a telecommunications network having an access server centrally configured between a traffic-bearing network and a plurality of network subsystems which control the provisioning and switching of available network resource, a method of allocating available bandwidth on the network comprising the steps of:

sending a user request for a telecommunications service;

intercepting the request at the access server level;

interpreting the request to determine the type of service requested by the user;

formatting the request according the a predetermined format compatible with said provisioning subsystem;

transmitting the formatted request to said provisioning subsystem;

determining if the user has authority to access the specified service; and

allocating enough network bandwidth to accommodate the request.

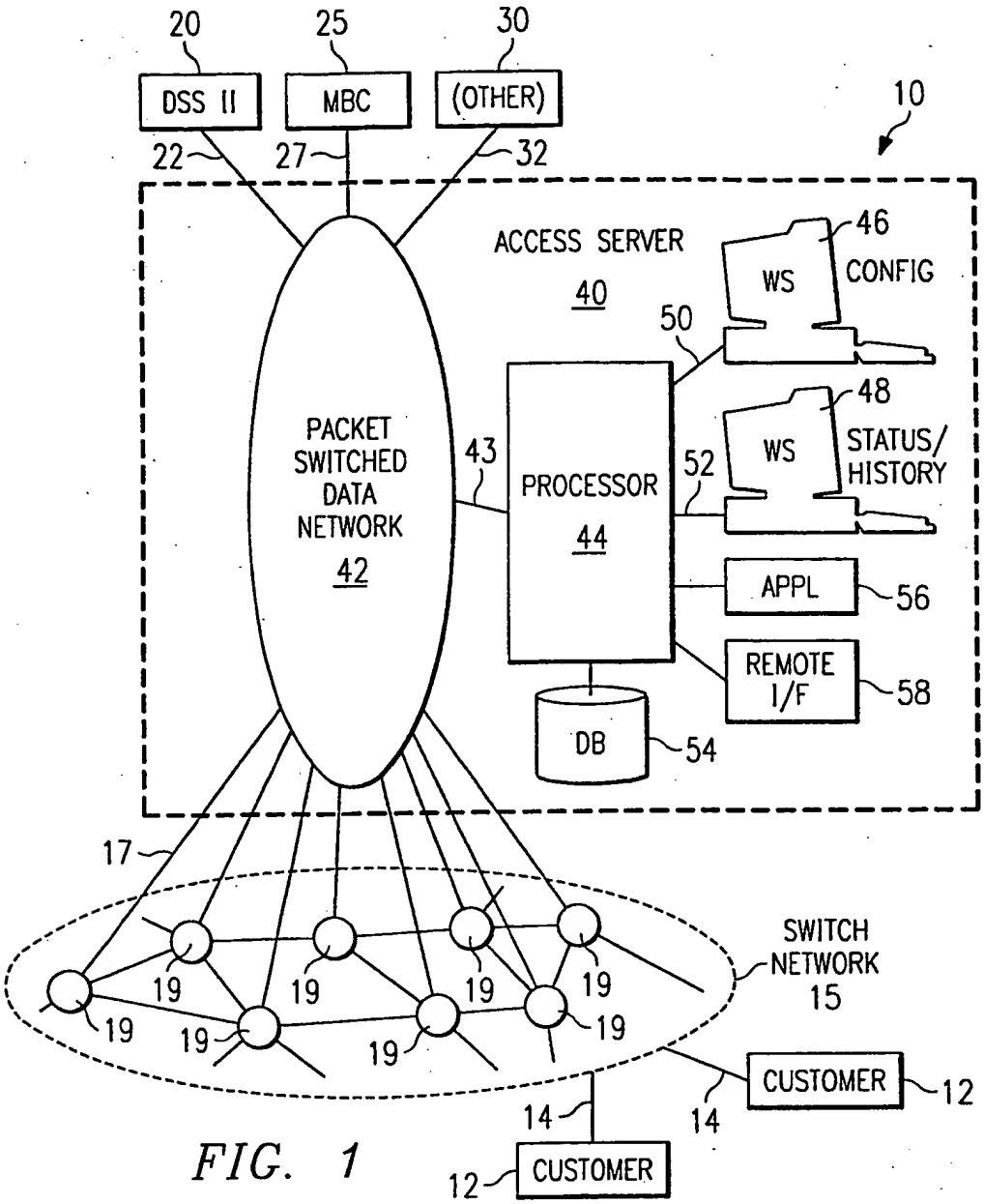

20
25
30
DSS II
MBC
(OTHER)
10
22
27
32
ACCESS SERVER
40
46
WS
CONFIG
50
48
WS
STATUS/
HISTORY
PACKET
SWITCHED
DATA
NETWORK
42
43
PROCESSOR
44
52
APPL
56
REMOTE
I/F
58
DB
54
17
19
SWITCH
NETWORK
15
CUSTOMER
12
14
14
CUSTOMER
12

FIG. 1

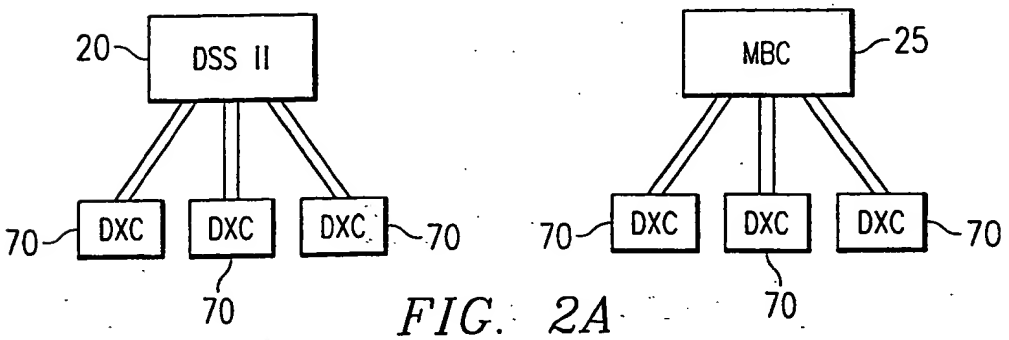

20
DSS II
25
MBC
70
DXC
DXC
DXC
70
70
70
DXC
DXC
DXC
70
70

FIG. 2A

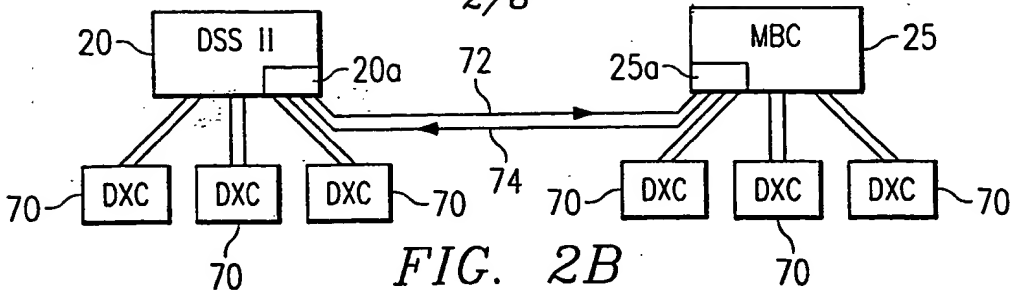


FIG. 2B

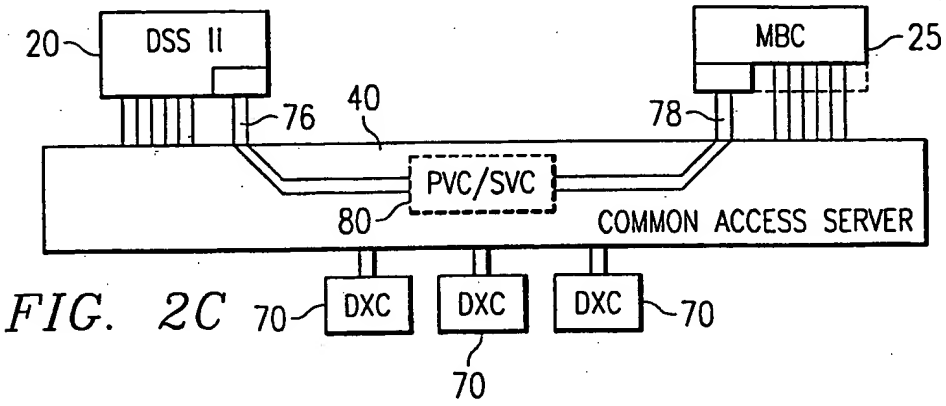


FIG. 2C

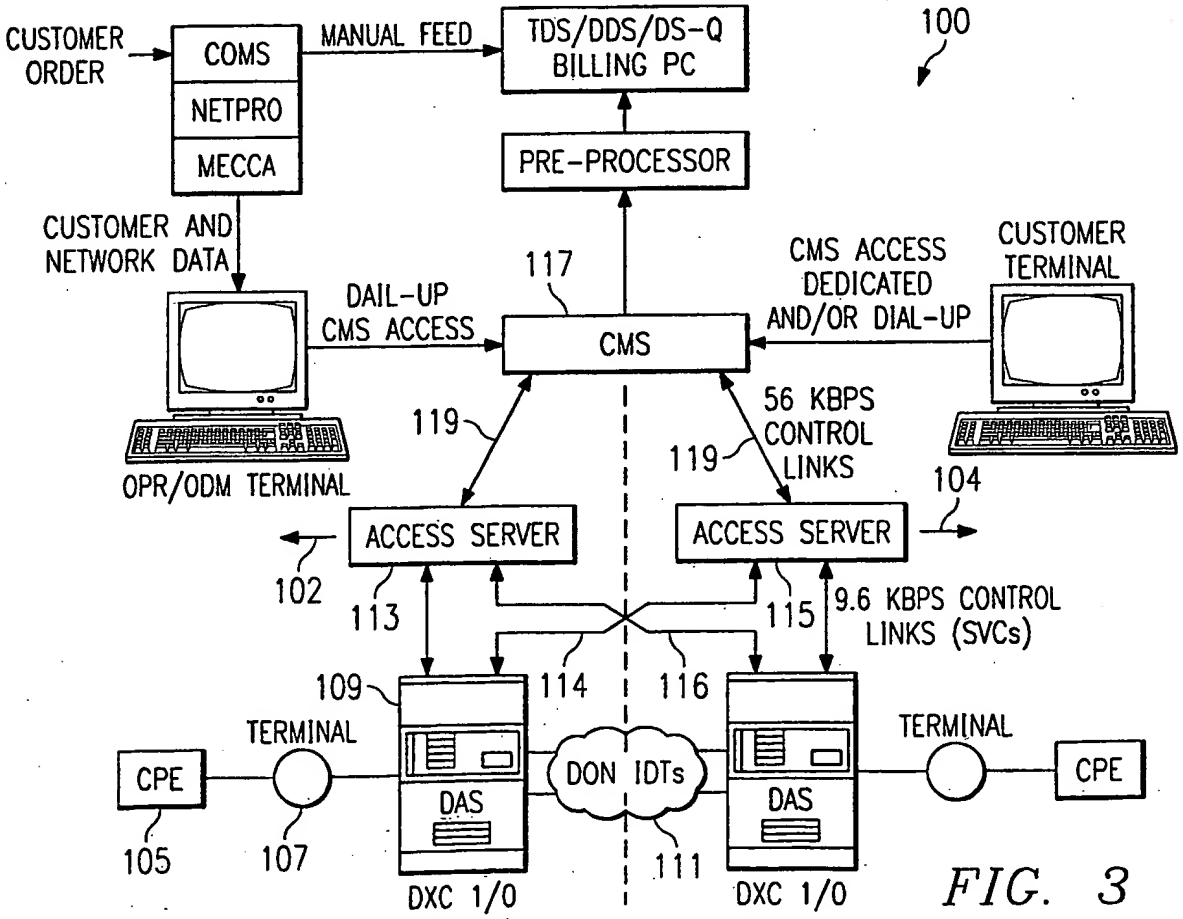


FIG. 3

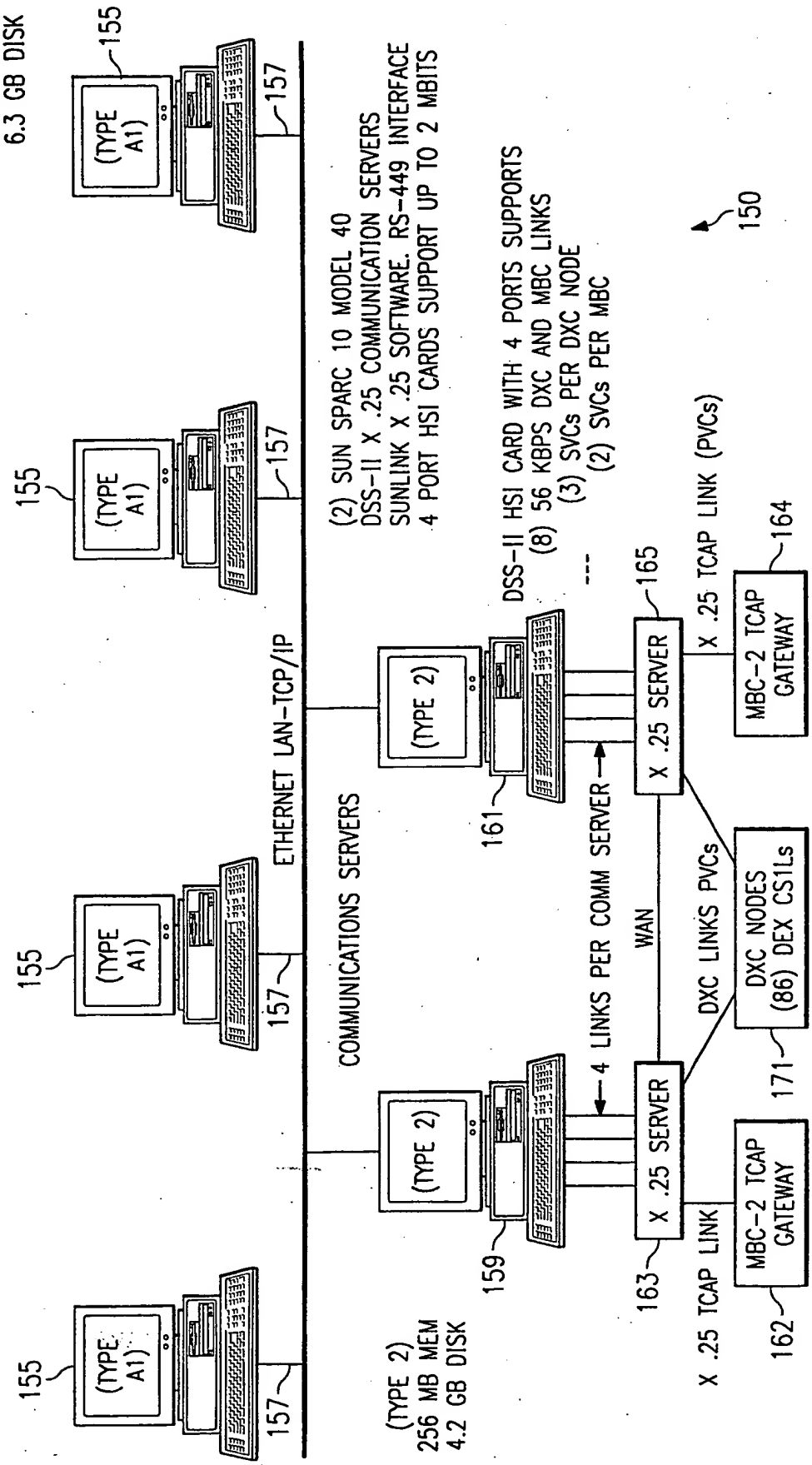

(TYPE A1)
256 MB MEM
6.3 GB DISK
155
157
(TYPE A1)
(2) SUN SPARC 10 MODEL 40
DSS-II X .25 COMMUNICATION SERVERS
SUNLINK X .25 SOFTWARE. RS-449 INTERFACE
4 PORT HSI CARDS SUPPORT UP TO 2 MBITS
ETHERNET LAN-TCP/IP
COMMUNICATIONS SERVERS
(TYPE 2)
DSS-II HSI CARD WITH 4 PORTS SUPPORTS
(8) 56 KBPS DXC AND MBC LINKS
(3) SVCs PER DXC NODE
(2) SVCs PER MBC
161
150
X .25 SERVER
165
X .25 TCAP LINK (PVCs)
MBC-2 TCAP GATEWAY
164
4 LINKS PER COMM SERVER
WAN
DXC LINKS PVCs
DXC NODES (86) DEX CS1Ls
171
(TYPE 2)
256 MB MEM
4.2 GB DISK
159
163
X .25 TCAP LINK
MBC-2 TCAP GATEWAY
162

FIG. 4

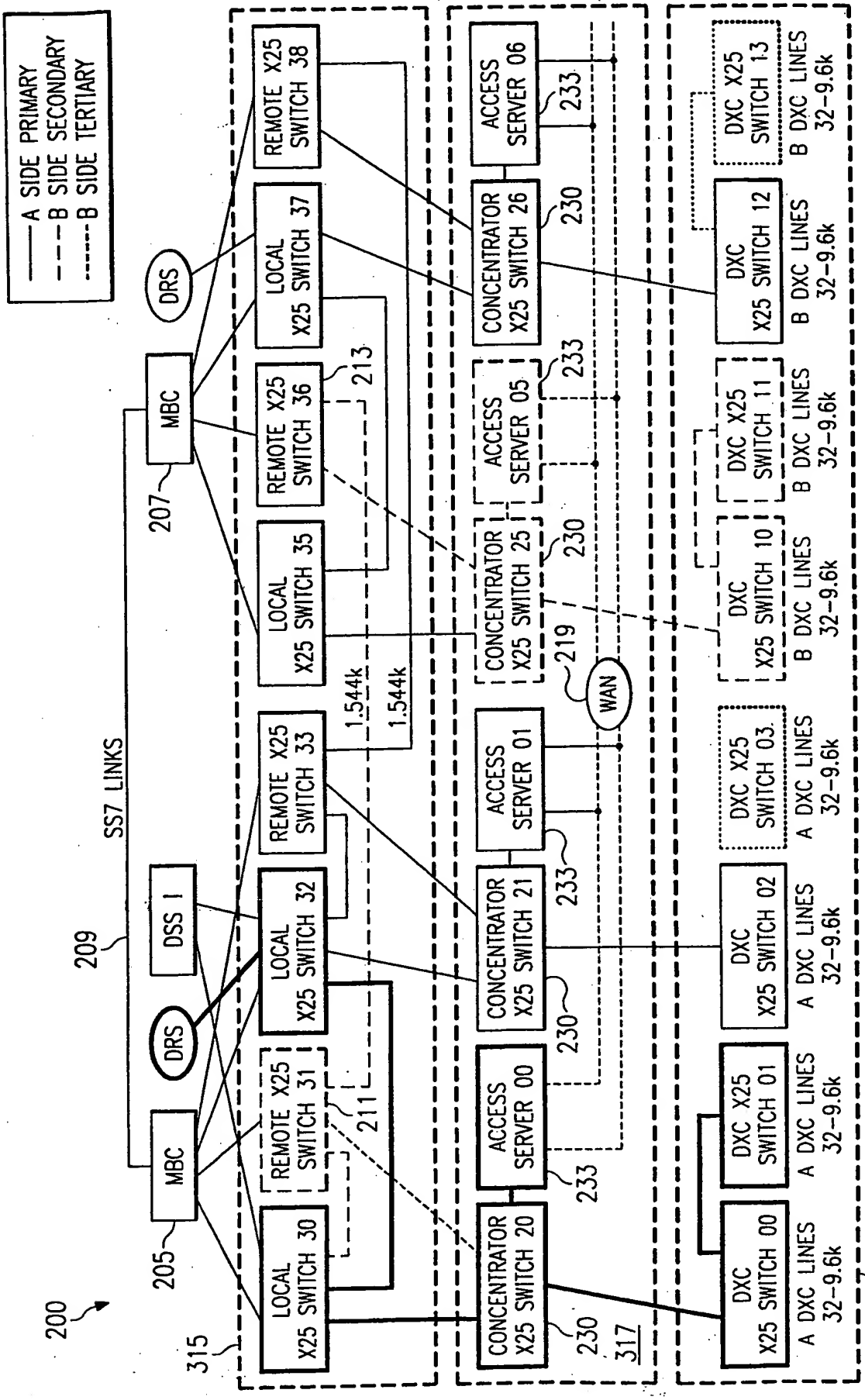

A SIDE PRIMARY
B SIDE SECONDARY
B SIDE TERTIARY
SS7 LINKS
MBC
DRS
DSS 1
LOCAL X25 SWITCH 30
LOCAL X25 SWITCH 32
LOCAL X25 SWITCH 35
LOCAL X25 SWITCH 37
REMOTE X25 SWITCH 31
REMOTE X25 SWITCH 33
REMOTE X25 SWITCH 36
REMOTE X25 SWITCH 38
CONCENTRATOR X25 SWITCH 20
CONCENTRATOR X25 SWITCH 21
CONCENTRATOR X25 SWITCH 25
CONCENTRATOR X25 SWITCH 26
ACCESS SERVER 00
ACCESS SERVER 01
ACCESS SERVER 05
ACCESS SERVER 06
DXC X25 SWITCH 00
DXC X25 SWITCH 01
DXC X25 SWITCH 02
DXC X25 SWITCH 03
DXC X25 SWITCH 10
DXC X25 SWITCH 11
DXC X25 SWITCH 12
DXC X25 SWITCH 13
A DXC LINES 32-9.6k
B DXC LINES 32-9.6k
WAN
1.544k
200
205
207
209
211
213
219
230
233
250
315
317

FIG. 5

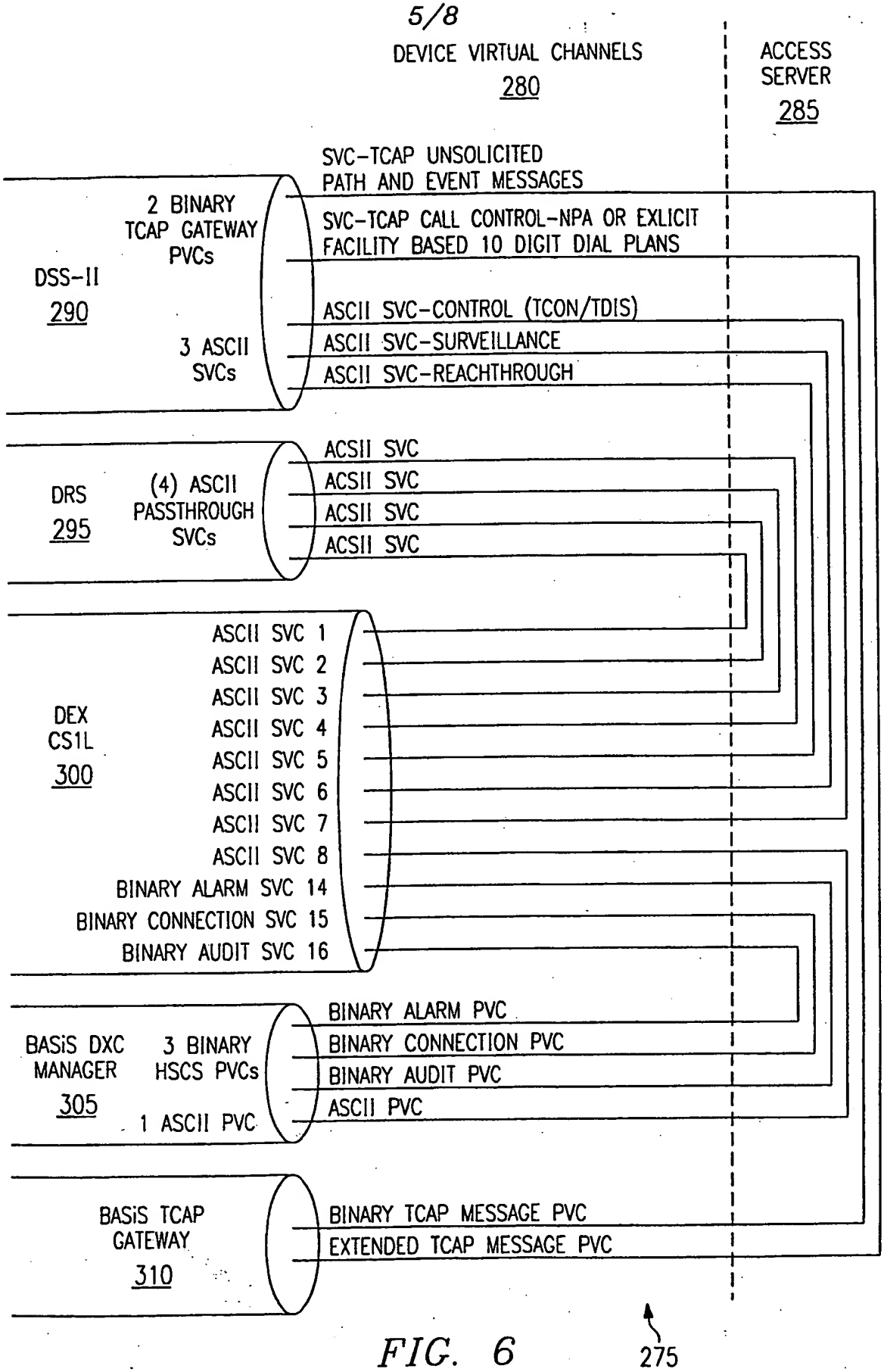

DEVICE VIRTUAL CHANNELS
280
ACCESS SERVER
285
SVC-TCAP UNSOLICITED PATH AND EVENT MESSAGES
SVC-TCAP CALL CONTROL-NPA OR EXLICIT FACILITY BASED 10 DIGIT DIAL PLANS
ASCII SVC-CONTROL (TCON/TDIS)
ASCII SVC-SURVEILLANCE
ASCII SVC-REACHTHROUGH
ACSII SVC
ACSII SVC
ACSII SVC
ACSII SVC
ASCII SVC 1
ASCII SVC 2
ASCII SVC 3
ASCII SVC 4
ASCII SVC 5
ASCII SVC 6
ASCII SVC 7
ASCII SVC 8
BINARY ALARM SVC 14
BINARY CONNECTION SVC 15
BINARY AUDIT SVC 16
BINARY ALARM PVC
BINARY CONNECTION PVC
BINARY AUDIT PVC
ASCII PVC
BINARY TCAP MESSAGE PVC
EXTENDED TCAP MESSAGE PVC
DSS-II
290
2 BINARY TCAP GATEWAY PVCs
3 ASCII SVCs
DRS
295
(4) ASCII PASSTHROUGH SVCs
DEX CS1L
300
BASiS DXC MANAGER
305
3 BINARY HSCS PVCs
1 ASCII PVC
BASiS TCAP GATEWAY
310
275

FIG. 6

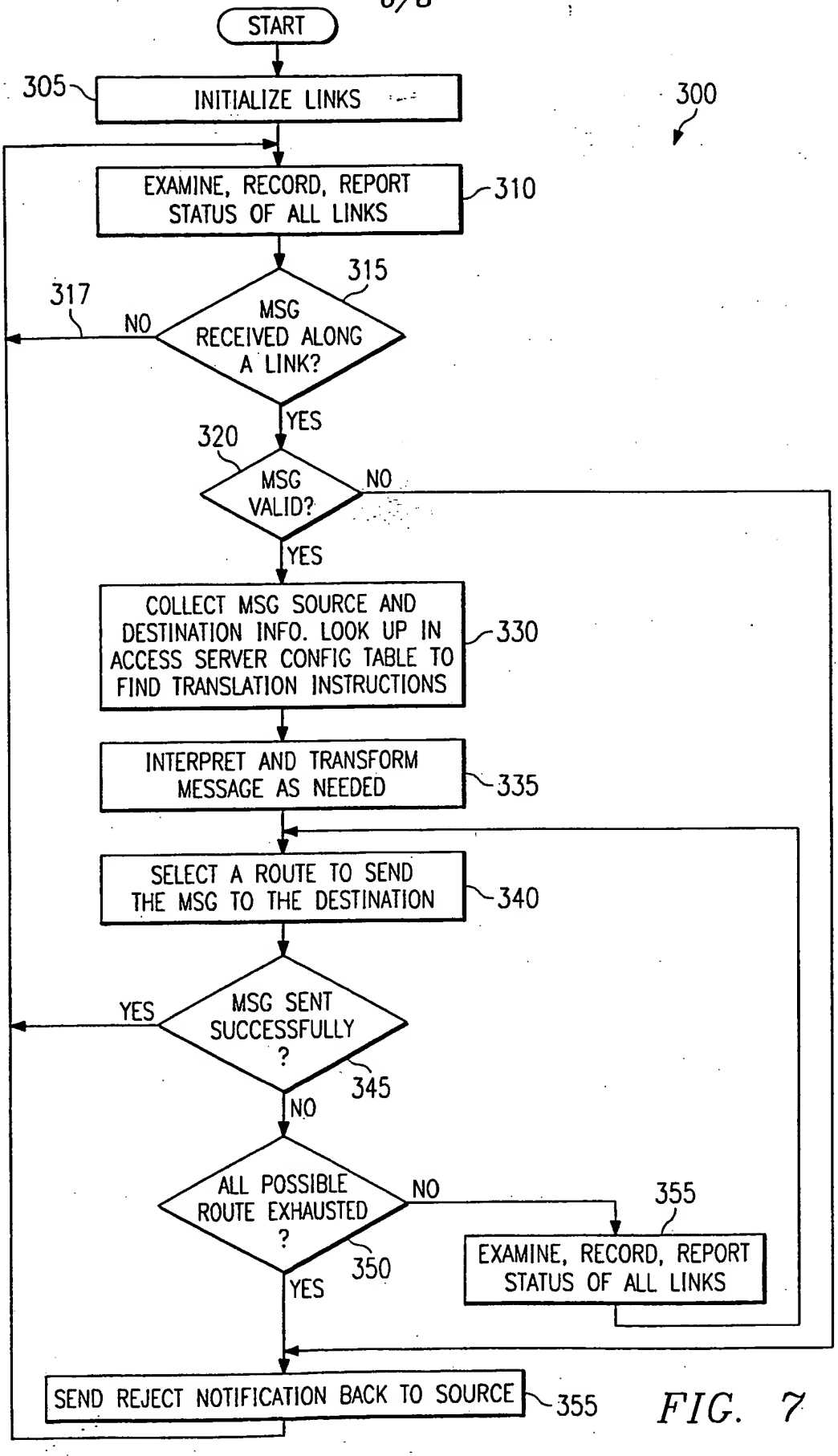

START
305
INITIALIZE LINKS
300
EXAMINE, RECORD, REPORT STATUS OF ALL LINKS
310
315
317
NO
MSG RECEIVED ALONG A LINK?
YES
320
MSG VALID?
NO
YES
COLLECT MSG SOURCE AND DESTINATION INFO. LOOK UP IN ACCESS SERVER CONFIG TABLE TO FIND TRANSLATION INSTRUCTIONS
330
INTERPRET AND TRANSFORM MESSAGE AS NEEDED
335
SELECT A ROUTE TO SEND THE MSG TO THE DESTINATION
340
YES
MSG SENT SUCCESSFULLY ?
345
NO
ALL POSSIBLE ROUTE EXHAUSTED ?
NO
355
350
YES
EXAMINE, RECORD, REPORT STATUS OF ALL LINKS
SEND REJECT NOTIFICATION BACK TO SOURCE
355

FIG. 7

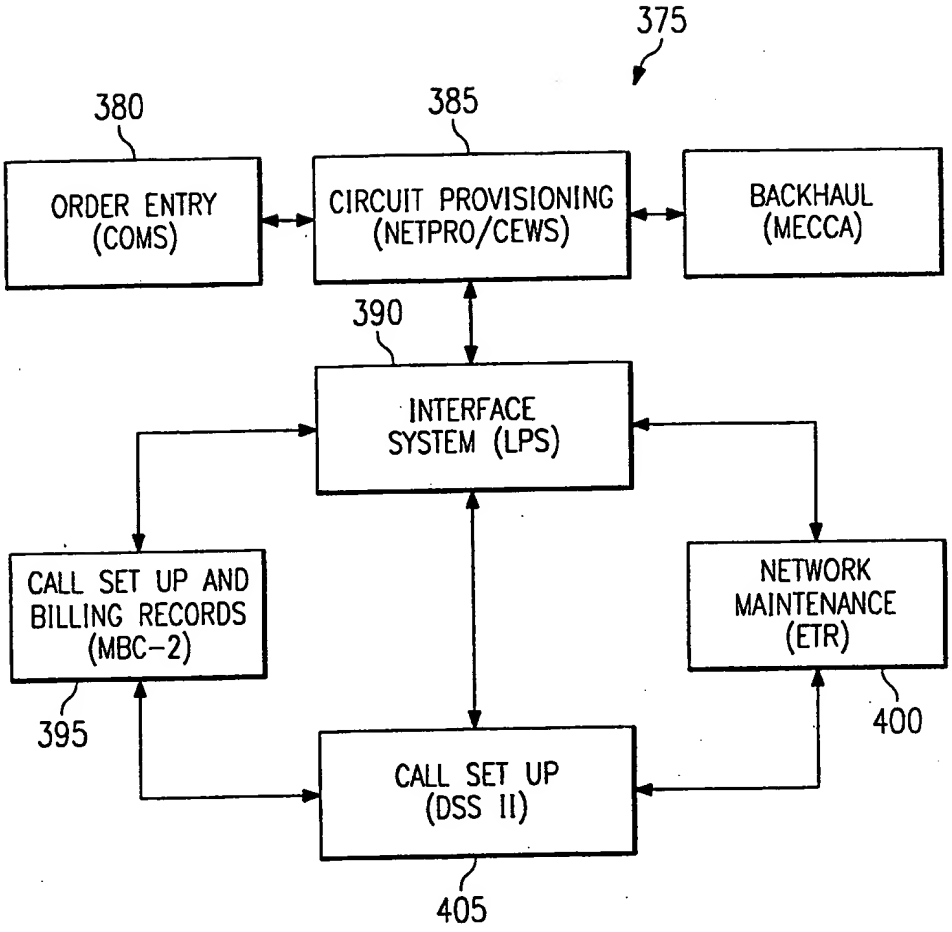

375
380
385
ORDER ENTRY (COMS)
CIRCUIT PROVISIONING (NETPRO/CEWS)
BACKHAUL (MECCA)
390
INTERFACE SYSTEM (LPS)
CALL SET UP AND BILLING RECORDS (MBC-2)
NETWORK MAINTENANCE (ETR)
395
400
CALL SET UP (DSS II)
405

FIG. 8

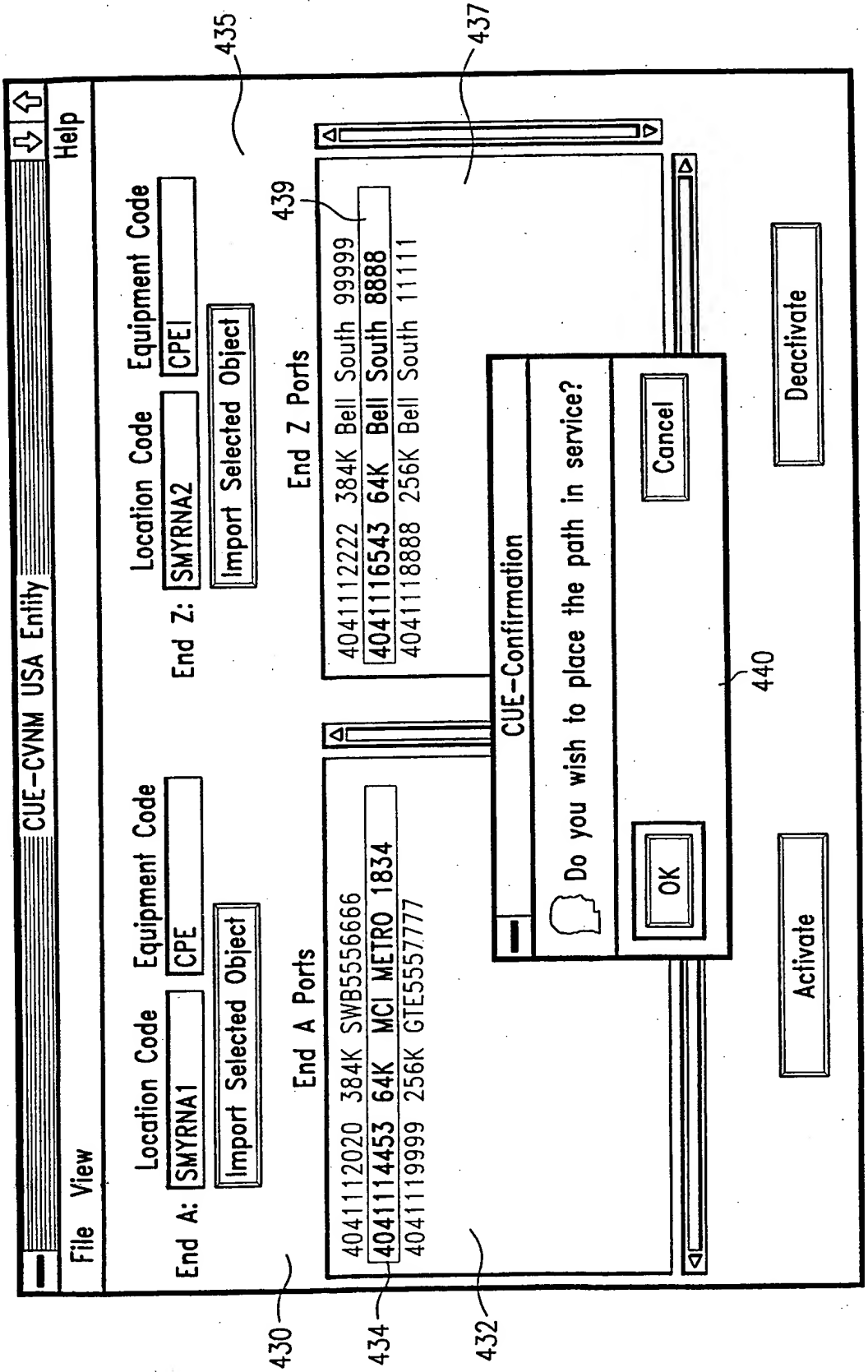

CUE-CVNM USA Entity
File View Help
End A:
Location Code
SMYRNA1
Equipment Code
CPE
Import Selected Object
End Z:
Location Code
SMYRNA2
Equipment Code
CPE1
Import Selected Object
End A Ports
4041112020 384K SWB5556666
4041114453 64K MCI METRO 1834
4041119999 256K GTE5557777
End Z Ports
4041112222 384K Bell South 99999
4041116543 64K Bell South 8888
4041118888 256K Bell South 11111
CUE-Confirmation
Do you wish to place the path in service?
OK
Cancel
Activate
Deactivate
430
434
432
435
437
439
440
425

FIG. 9

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/US 97/19223

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 07281 A (BRITISH TELECOMM ;AZARMI NADER (GB); CORLEY STEPHEN LESLIE (GB)) 7 March 1996	1,3,12
Y	see abstract	5
A	see figures 1,3,6,11 see page 11, line 9 - page 14, line 4 see page 25, line 14 - page 27, line 17	2,4,6-11
Y	COX W V: "THE FLEXCOM TM/LINC SYSTEM: A CUSTOMER NETWORK RECONFIGURATION SYSTEM" COMMUNICATIONS: CONNECTING THE FUTURE, SAN DIEGO, DEC. 2- 5, 1990, vol. 1 OF 3, 2 December 1990., INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, pages 72-75, XP000218699	5
A	see the whole document	1-4,6-12

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 January 1998	03/02/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cichra, M

INTERNATIONAL SEARCH REPORT

Ir tional Application No
PCT/US 97/19223

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 95 24802 A (BRITISH TELECOMM ;COX SIMON ANDREW (GB); GITTINS CHRISTOPHER JOHN) 14 September 1995 see abstract see page 6, line 4 - page 7, line 33 see figures 4-6 see claims 1,2	1-12
A	GAWLICK R ET AL: "On-line routing for permanent virtual circuits" COMPUTER COMMUNICATIONS, vol. 19, no. 3, March 1996, page 235-244 XP004032406 see the whole document	1,3,4, 10-12
A	EP 0 658 062 A (AT & T CORP) 14 June 1995 see the whole document	1,5-7,9, 11,12
A	CAMPBELL R C ET AL: "AT&T AGGRESSIVELY MOVES ISDN FORWARD" AT & T TECHNOLOGY, vol. 6, no. 1, 1 January 1991, pages 22-29, XP000235018 see the whole document	1,3, 10-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int tional Application No
PCT/US 97/19223

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9607281 A	07-03-96	AU 3393595 A	22-03-96
		CA 2198885 A	07-03-96
		EP 0786187 A	30-07-97
		FI 970849 A	25-04-97
		NO 970943 A	28-04-97
		NZ 292213 A	26-05-97
WO 9524802 A	14-09-95	AU 1856395 A	25-09-95
		EP 0749662 A	27-12-96
		JP 9510064 T	07-10-97
		US 5499240 A	12-03-96
		US 5638363 A	10-06-97
		US 5526350 A	11-06-96
EP 0658062 A	14-06-95	US 5440563 A	08-08-95
		CA 2123347 A	13-04-95
		CN 1110461 A	18-10-95
		JP 7177147 A	14-07-95

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)